IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE:	MDL Docket No 06-1791 VRW
NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	ORDER

____

This order pertains to:

Al-Haramain Islamic Foundation et al v Bush et al (C 07-0109 VRW),
_____________________________________/

On November 16, 2007, the court of appeals remanded this case for this court to consider whether the Foreign Intelligence Surveillance Act, 50 USC §§ 1801-71, ("FISA") "preempts the state secrets privilege and for any proceedings collateral to that determination." Al-Haramain Islamic Foundation, Inc v Bush, 507 F3d 1190, 1206 (9th Cir 2007). This court entertained briefing and held a hearing on that issue and, on July 2, 2008, issued a ruling that: (1) FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes and would appear to displace the state secrets privilege for purposes of plaintiffs' claims; and (2) FISA did not appear to provide plaintiffs with a viable remedy unless they could show that they were "aggrieved persons" within the meaning of FISA. In re

National Security Agency Telecommunications Records Litigation, 564 F Supp 2d 1109, 1111 (N D Cal 2008). The court dismissed the complaint with leave to amend. Plaintiffs timely filed an amended pleading (Doc #458/35[1]) and defendants, for the third time, moved to dismiss (Doc #475/49). Plaintiffs simultaneously filed a motion to "discover or obtain material relating to electronic surveillance" under 50 USC § 1806(f) (Doc #472/46), which defendants oppose (Doc #496/50).

This pair of cross-motions picks up, at least in theory, where the court's July 2, 2008 order left off. At issue on these cross-motions is the adequacy of the first amended complaint (Doc #35/458)("FAC") to enable plaintiffs to proceed with their suit. Accordingly, the court's discussion will address the motions together.[2]

I

As with the original complaint, plaintiffs are the Al-Haramain Islamic Foundation, Inc, an Oregon non-profit corporation ("Al-Haramain Oregon"), and two of its individual attorneys, Wendell Belew and Asim Ghafoor, both United States citizens ("plaintiffs"). Plaintiffs sue generally the same defendants but replace one office-holder with his replacement, make minor punctuation and wording changes and specify that they are suing one

[1] Documents will cited both to the MDL docket number (No M 06-1791) and to the individual docket number (No C 07-0109) in the following format: Doc #xxx/yy.

[2] These motions do not implicate the recent amendments to FISA enacted after the July 2 order (FISA Amendments Act of 2008, Pub L No 110-261, 122 Stat 2436 (FISAAA), enacted July 10, 2008).

defendant in both his official and personal capacities: "George W Bush, President of the United States, National Security Agency and Keith B Alexander, its Director; Office of Foreign Assets Control, an office of the United States Treasury, and Adam J Szubin, its Director; Federal Bureau of Investigation and Robert S Mueller, III, its Director, in his official and personal capacities" ("defendants").

The FAC retains the same six causes of action as the original complaint. First, plaintiffs allege a cause of action under FISA that encompasses both a request, under 50 USC § 1806(g), for suppression of evidence obtained through warrantless electronic surveillance and a claim for damages under § 1810. Doc #458/35 at 14. Then, plaintiffs allege violations of the following Constitutional provisions: the "separation of powers" principle (i e, that the executive branch has exceeded its authority under Article II); the Fourth Amendment through warrantless surveillance of plaintiffs' electronic communications; the First Amendment through warrantless surveillance, impairing plaintiffs' "ability to obtain legal advice, to freely form attorney-client relationships, and to petition the government * * * for redress of grievances * * *"; and the Sixth Amendment through surveillance of plaintiffs' electronic communications without probable cause or warrants. Id at 14-15. And finally, plaintiffs allege violations of the International Covenant on Civil and Political Rights. Id at 15-16.

In drafting the FAC, plaintiffs have greatly expanded their factual recitation, which now runs to ten pages (id at 3-12), up from a little over one page. The FAC recites in considerable detail a number of public pronouncements of government officials about the Terrorist Surveillance Project ("TSP") and its surveillance activities as well as events publicly known about the TSP including a much-publicized hospital room confrontation between former Attorney General John Ashcroft and then-White House counsel (later Attorney General) Alberto Gonzales (id at 5).

Of more specific relevance to plaintiffs' effort to allege sufficient facts to establish their "aggrieved person" status, the FAC also recites a sequence of events pertaining directly to the government's investigations of Al-Haramain Oregon. A slightly abbreviated version of these allegations follows:

On August 1, 2002, Treasury Department Deputy Secretary Kenneth W Dam testified in Congress that, in October of 2001, the Treasury Department created "Operation Green Quest" to track financing of terrorist activities, one of the targets of which were foreign branches of the Saudi Arabia-based Al-Haramain Islamic Foundation. ¶ 24.

On March 4, 2004, FBI Counterterrorism Division Acting Assistant Director Gary M Bald testified in Congress that: in April of 2002, the FBI created its Terrorist Financing Operations Section (TFOS); on May 13, 2003, through a Memorandum of Understanding between the Department of Justice and the Department of Homeland Security, the FBI was designated as the lead Department to investigate potential terrorist-related financial transactions; the TFOS acquired, analyzed and disseminated classified electronic intelligence data, including telecommunications data from sources in government and private industry; TFOS took over the investigation of Al-Haramain Islamic Foundation "pertaining to terrorist financing"; on February 18, 2004, the FBI executed a search warrant on plaintiff Al-Haramain Oregon's office in Ashland, Oregon; and TFOS provided operational support, including document and data analysis, in the investigation of plaintiff Al-Haramain Oregon. ¶ 25. Bald's March 4, 2004 testimony included no mention of purported links between plaintiff Al-Haramain Oregon and Osama bin-Laden. ¶ 26.

On September 25, 2003, FBI Deputy Director John S Pistole testified in Congress that the TFOS "has access to data and information" from "the Intelligence Community" and has "[t]he ability to access and obtain this type of information in a time sensitive and urgent manner." ¶ 27.

On June 16, 2004, OFAC Director R Richard Newcomb testified in Congress that in conducting investigations of terrorist financing, OFAC officers use "classified * * * information sources." ¶ 28.

On July 26, 2007, defendant Mueller testified before the House Judiciary Committee that in 2004 the FBI, under his direction, undertook activity using information produced by the NSA through the warrantless surveillance program.

On February 19, 2004, the Treasury Department issued a press release announcing that OFAC had blocked Al-Haramain Oregon's assets pending an investigation of possible crimes relating to currency reporting and tax laws; the document contained no mention of purported links between plaintiff Al-Haramain Oregon and Osama bin-Laden. ¶¶ 30-31.

Soon after the blocking of plaintiff Al-Haramain Oregon's assets on February 19, 2004, plaintiff Belew spoke by telephone with Soliman al-Buthi (alleged to be one of Al-Haramain Oregon's directors) on the following dates: March 10, 11 and 25, April 16, May 13, 22 and 26, and June 1, 2 and 10, 2004. Belew was located in Washington DC; al-Buthi was located in Riyadh, Saudi Arabia. During the same period, plaintiff Ghafoor spoke by telephone with al-Buthi approximately daily from February 19 through February 29, 2004 and approximately weekly thereafter. Ghafoor was located in Washington DC; al-Buthi was located in Riyadh, Saudi Arabia. (The FAC includes the telephone numbers used in the telephone calls referred to in this paragraph.) ¶¶ 34-35.

In the telephone conversations between Belew and al-Buthi, the parties discussed issues relating to the legal representation of defendants, including Al-Haramain Oregon, named in a lawsuit brought by victims of the September 11, 2001 attacks. Names al-Buthi mentioned in the telephone conversations with Ghafoor included Mohammad Jamal Khalifa, who was married to one of Osama bin-Laden's sisters, and Safar al-Hawali and Salman al-Auda, clerics whom Osama bin-Laden claimed had inspired him. In the telephone conversations between Ghafoor and al-Buthi, the parties also discussed logistical issues relating to payment of Ghafoor's legal fees as defense counsel in the lawsuit. Id.

In a letter to Al-Haramain Oregon's lawyer Lynne Bernabei dated April 23, 2004, OFAC Director Newcomb stated that OFAC was considering designating Al-Haramain Oregon as a Specially Designated Global Terrorist (SDGT) organization based on unclassified information "and on classified documents that are not authorized for public disclosure." ¶ 36. In a follow-up letter to Bernabei dated July 23, 2004, Newcomb reiterated that OFAC was considering "classified information not being provided to you" in determining whether to designate Al-Haramain Oregon as an SDGT organization. ¶ 37. On September 9, 2004, OFAC declared plaintiff Al-Haramain Oregon to be an SDGT organization. ¶ 38.

In a press release issued on September 9, 2004, the Treasury Department stated that the investigation of Al-Haramain Oregon showed "direct links between the US branch [of Al-Haramain] and Usama bin Laden"; this was the first public claim of purported links between Al-Haramain Oregon and Osama bin-Laden. ¶¶ 39-40.

In a public declaration filed in this litigation dated May 10, 2006, FBI Special Agent Frances R Hourihan stated that a classified document "was related to the terrorist designation" of Al-Haramain Oregon.

On October 22, 2007, in a speech at a conference of the American Bankers Association and American Bar Association on money laundering, the text of which appears on the FBI's official Internet website, FBI Deputy Director Pistole stated that the FBI "used * * * surveillance" in connection with defendant OFAC's 2004 investigation of Al-Haramain Oregon but that "it was the financial evidence" provided by financial institutions "that provided justification for the initial designation" of Al-Haramain Oregon. ¶¶ 42-43. A court document filed by the United States Attorney for the District of Oregon on August 21, 2007 referred to the February 19, 2004 asset-blocking order as a "preliminary designation" and the September 9, 2004 order as "a formal designation." ¶ 44.

To allege that the above-referenced telecommunications between al-Buthi and plaintiffs Belew and Ghafoor were wire communications and were intercepted by defendants within the United States, plaintiffs cite in their FAC several public statements by government officials, including: July 26, 2006 testimony by defendant Alexander and CIA Director Michael Hayden that telecommunications between the United States and abroad pass through routing stations located within the United States from which the NSA intercepts such telecommunications; May 1, 2007 testimony by Director of National Intelligence Mike McConnell that interception of surveilled electronic communications between the United States and abroad occurs within the United States and thus requires a warrant under FISA; September 20, 2007 testimony by McConnell testified before the House Select Intelligence Committee that "[t]oday * * * [m]ost international communications are on a wire, fiber optical cable," and "on a wire, in the United States, equals a warrant requirement [under FISA] even if it was against a foreign person located overseas." ¶ 48a-c.

A memorandum dated February 6, 2008, to defendant Szubin from Treasury Department Office of Intelligence and Analysis Deputy Assistant Secretary Howard Mendelsohn, which was publicly disclosed during a 2005 trial, acknowledged electronic surveillance of four of Al-Buthi's telephone calls with an individual unrelated to this case on February 1, 2003. ¶ 51.

In support of their motion under § 1806(f), plaintiffs submit evidence substantiating the allegations of their FAC. In addition to numerous documents drawn from United States government websites and the websites of news organizations (Exhibits to Doc #472-1/46-1, passim), plaintiffs submit the sworn declarations of plaintiffs Wendell Belew and Asim Ghafoor attesting to the specifics and contents of the telephone conversations described in paragraphs 32 and 33 of the FAC. Doc ##472-6/46-6, 472-7/46-7.

II

Defendants' papers attack the sufficiency of plaintiffs' allegations in their FAC and the evidence presented in their motion under § 1806(f) to establish that they are "aggrieved persons" under FISA and thereby have standing to utilize the special procedures set forth in § 1806(f) of FISA to investigate the alleged warrantless surveillance and to seek civil remedies under § 1810. An "aggrieved person" under FISA is defined in 50 USC §1801(k) as the "target of an electronic surveillance" or a person "whose communications or activities were subject to electronic surveillance." Defendants contend that "nothing in the [FAC] comes close to establishing that plaintiffs are 'aggrieved persons' under FISA and thus have standing to proceed under Section 1806(f) to litigate any claim." Doc #475/49 at 6.

Plaintiffs' motion, by contrast, asserts that the FAC presents "abundant unclassified information demonstrating plaintiffs' electronic surveillance in March and April of 2004" and, on that basis, seeks a determination of "aggrieved person" status under FISA. Plaintiffs also "propose several possible security measures by which plaintiffs can safely be given access to portions of" the classified document that was accidentally revealed to plaintiffs during discovery and returned under orders of the Oregon District Court (the "Sealed Document") and which has been the subject of considerable attention in this litigation. Doc #472/46 at 5-6.

\\

\\

\\

A

Both FISA sections under which plaintiffs seek to proceed, §§ 1810 and 1806(f), are available only to "aggrieved persons" as defined in 50 USC § 1801(k). The court's July 2 order discussed the lack of precedents under FISA and devoted considerable space to opinions applying 18 USC § 3504(a)(1), governing litigation concerning sources of evidence. 564 F Supp 2d at 1133-35. The Ninth Circuit's standards under § 3504(a)(1), while not directly transferrable to FISA, appear to afford a source of relevant analysis to use by analogy in interpreting FISA, subject to that statute's national-security-oriented context:

> The flexible or case-specific standards articulated by the Ninth Circuit for establishing aggrieved status under section 3504(a)(1), while certainly relevant, do not appear directly transferrable to the standing inquiry for an "aggrieved person" under FISA. While attempting a precise definition of such a standard is beyond the scope of this order, it is certain that plaintiffs' showing thus far with the Sealed Document excluded falls short of the mark.
>
> Plaintiff amici hint at the proper showing when they refer to "independent evidence disclosing that plaintiffs have been surveilled" and a "rich lode of disclosure to support their claims" in various of the MDL cases. ***
>
> To proceed with their FISA claim, plaintiffs must present to the court enough specifics based on non-classified evidence to establish their "aggrieved person" status under FISA.

Id at 1135.

Defendants' opening brief (Doc #475/49) largely fails to engage with the question posed by the court, instead reiterating standing arguments made previously (at 16-17) and asserting that "the law does not support an attempt to adjudicate whether the plaintiffs are 'aggrieved persons' in the face of the Government's successful state secrets privilege assertion" (at 27-30).

United States District Court
For the Northern District of California

Defendants advance one apparently new argument in this regard: that the adjudication of "aggrieved person" status for any or all plaintiffs cannot be accomplished without revealing information protected by the state secrets privilege ("SSP"). This argument rests on the unsupported assertion that "[t]he Court cannot exercise jurisdiction based on anything less than the actual facts" (id at 28), presumably in contrast to inferences from other facts (on which defendants contend the FAC exclusively relies). Defendants' position boils down to this: only affirmative confirmation by the government or equally probative evidence will meet the "aggrieved person" test; the government is not required to confirm surveillance and the information is not otherwise available without invading the SSP. In defendants' view, therefore, plaintiffs simply cannot proceed on their claim without the government's active cooperation —— and the government has evinced no intention of cooperating here.

Defendants' stance does not acknowledge the court's ruling in the July 2, 2008 order that FISA "preempts" or displaces the SSP for matters within its purview and that, while obstacles abound, canons of construction require that the court avoid interpreting and applying FISA in a way that renders FISA's § 1810 superfluous. Accordingly, the court ruled, there must be some legally sufficient way to allege that one is an "aggrieved person" under § 1801(k) so as to survive a motion to dismiss. Of note, defendants also continue to maintain, notwithstanding the July 2 rulings, that the SSP requires dismissal and that FISA does not preempt the SSP. They also suggest that appellate review of the preemption ruling and several of the issues implicated in the instant motions might be "appropriate" if the court decides to proceed under § 1806(f). Doc #475/49 at 31. (Plaintiffs counter that an interlocutory appeal of the preemption question would not be timely. Doc #496/50 at 28).

Plaintiffs urge the court to adopt the Ninth Circuit's prima facie approach under 18 USC § 3504(a)(1) set forth in United States v Alter, 482 F2d 1016 (9th Cir 1973), that is, that a prima facie case of electronic surveillance requires "evidence specifically connecting them with the surveillance —— i e showing that they were surveilled" without requiring that they "plead and prove [their] entire case." Plaintiffs further suggest that the prima facie case does not require the determination of any contested facts but rather is "a one-sided affair —— the plaintiff's side." Doc #472/46 at 20.

Plaintiffs also point to the DC Circuit's recent decision in In Re Sealed Case, 494 F 3d 139 (DC Cir 2007), which reversed the district court's dismissal of a Bivens action by a Drug Enforcement Agency employee based on the government's assertion of the SSP. The district court had concluded that the plaintiff's unclassified allegations of electronic eavesdropping in violation of the Fourth Amendment were insufficient to establish a prima facie case. Id at 147. The DC Circuit upheld the dismissal as to a defendant called "Defendant II" of whom the court wrote "nothing about this person would be admissible in evidence at trial," but reversed the dismissal as to defendant Huddle, noting that although plaintiff's case "is premised on circumstantial evidence 'as in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence.'" Id. Plaintiffs accordingly argue that circumstantial evidence of electronic surveillance should be sufficient to establish a prima facie case. The court agrees with plaintiffs that this approach comports with the intent of Congress in enacting FISA as well as concepts of due process which are especially challenging —— but nonetheless especially important —— to uphold in cases with national security implications and classified evidence.

Plaintiffs articulate their proposed standard, in summary, as follows: "plaintiffs' burden of proving their 'aggrieved person' status is to produce unclassified prima facie evidence, direct and/or circumstantial, sufficient to raise a reasonable inference on a preponderance of the evidence that they were subjected to electronic surveillance." Doc #472/46 at 19.

Defendants attack plaintiffs' proposed prima facie case approach by suggesting, as to plaintiffs' motion, that "no court has ever used Section 1806(f) in this manner" and that it would "open a floodgate of litigation whereby anyone who believes he can 'infer' from 'circumstantial evidence' that he was subject to electronic surveillance could compel a response by the Attorney General under Section 1806(f) and seek discovery of the matter through ex parte, in camera proceedings." Doc # 499/51 at 12-13. These points are without merit.

The lack of precedents for plaintiffs' proposed approach is not meaningful given the low volume of FISA litigation in the thirty years since FISA was first enacted. It is, moreover, unlikely that this court's order allowing plaintiffs to proceed will prompt a "flood" of litigants to initiate FISA litigation as a means of learning about suspected unlawful surveillance of them by the government. And finally, the court has ruled that allegations sufficient to allege electronic surveillance under FISA must be, to some degree, particularized and specific, a ruling that discourages weakly-supported claims of electronic surveillance. In re National Security Agency, 564 F Supp 2d at 1135.

In Alter, the Ninth Circuit specifically noted the competing considerations and special challenges for courts in cases of alleged electronic surveillance:

> We * * * seek to create a sound balance among the competing demands of constitutional safeguards protecting the witness and the need for orderly grand jury processing. We do not overlook the intrinsic difficulty in identifying the owner of an invisible ear; nor do we discount the need to protect the Government from unwarranted burdens in responding to ill-founded suspicions of electronic surveillance.

482 F2d at 1026. The prima facie approach employed by the Ninth Circuit fairly balances the important competing considerations at work in electronic surveillance cases. Its stringency makes it appropriate in cases arising in the somewhat more restrictive litigation environment where national security dimensions are present. The DC Circuit's recent use of a prima facie approach in such a case underscores that this is a proper manner in which to proceed. In re Sealed Case,494 F 3d 139. It appears consistent, moreover, with the intent of Congress in enacting FISA's sections 1810 and 1806(f).

B

Defendants devote considerable space to their argument that plaintiffs have not established "Article III standing." E g, Doc #475/49 at 17. In support of this contention, they largely rehash and re-purpose the standing arguments made in support of their previous two motions to dismiss.

The court will limit its discussion of this issue to defendants' reliance on Alderman v United States, 394 US 165 (1969), which they cite in all of their briefs on these motions in support of their contention that plaintiffs lack standing. Doc #475/49 at 17; Doc # 499/51 at 9, 10, 26 and 27; Doc #516/54 at 9. In Alderman, the Supreme Court considered, in connection with legal challenges brought under the Fourth Amendment, "the question of standing to object to the Government's use of the fruits of illegal surveillance" in criminal prosecutions. Id at 169. Explaining that "[w]e adhere to * * * the general rule that Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted," the Court held that the Fourth Amendment protects not only the private conversations of individuals subjected to illegal electronic surveillance, but also the owner of the premises upon which the surveillance occurs. While the Court made mention of the then-recently-enacted **Omnibus Crime Control and Safe Streets Act of 1968 codified at chapter 119 of Title 18 of the United States Code, 18 USC §§ 2510-22** ("Title III"), Alderman did not arise under Title III.

The footnote about standing that defendants repeatedly cite on the instant motions merely amplified the statement in the text of Alderman that "Congress or state legislatures may extend the exclusionary rule and provide that illegally seized evidence is inadmissible against anyone for any purpose," with the observation that Congress had not provided for such an expansion of standing to suppress illegally intercepted communications in Title III. Id at

175 & n9. Defendants' reliance on Alderman is somewhat baffling because here, the individuals who were allegedly subjected to the warrantless electronic surveillance are parties to the lawsuit and are specifically seeking relief under provisions of FISA intended to provide remedies to individuals subjected to warrantless electronic surveillance. The disposition in Alderman further undermines defendants' broader contention that only acknowledged warrantless surveillance confers standing: the Court remanded the cases to the district court for "a hearing, findings, and conclusions" whether there was electronic surveillance that violated the Fourth Amendment rights of any of the petitioners and, if so, as to the relevance of the surveillance evidence to the criminal conviction at issue. Id at 186.

The court declines to entertain further challenges to plaintiffs' standing; the July 2 order (at 1137) gave plaintiffs the opportunity to "amend their claim to establish that they are 'aggrieved persons' within the meaning of 50 USC § 1801(k)." Plaintiffs have alleged sufficient facts to withstand the government's motion to dismiss. To quote the Ninth Circuit in Alter, "[t]he [plaintiff] does not have to plead and prove his entire case to establish standing and to trigger the government's responsibility to affirm or deny." 482 F2d at 1026. Contrary to defendants' assertions, proof of plaintiffs' claims is not necessary at this stage. The court has determined that the allegations "are sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented." Id at 1025.

\\

C

Defendants summarize plaintiffs' allegations thusly, asserting that they are "obviously" insufficient "under any standard":

> the sum and substance of plaintiffs' factual allegations are that: (i) the [TSP] targeted communications with individuals reasonably believed to be associated with al Qaeda; (ii) in February 2004, the Government blocked the assets of AHIF-Oregon based on its association with terrorist organizations; (iii) in March and April of 2004, plaintiffs Belew and Ghafoor talked on the phone with an officer of AHIF-Oregon in Saudi Arabia (Mr al-Buthe [sic]) about, inter alia, persons linked to bin-Laden; (iv) in the September 2004 designation of AHIF-Oregon, [OFAC] cited the organization's direct links to bin-Laden as a basis for the designation; (v) the OFAC designation was based in part on classified evidence; and (vi) the FBI stated it had used surveillance in an investigation of the Al-Haramain Islamic Foundation. Plaintiffs specifically allege that interception of their conversations in March and April 2004 formed the basis of the September 2004 designation, and that any such interception was electronic surveillance as defined by the FISA conducted without a warrant under the TSP.

Doc #516/54 at 12 (citations to briefs omitted).

The court does not find fault with defendants' summary but disagrees with defendants' sense of the applicable legal standard. Defendants seem to agree that legislative history and precedents defining "aggrieved person" from the Title III context may be relevant to the FISA context (Doc #475/49 at 17 n 3), but argue that "Congress incorporated Article III standing requirements in any determination as to whether a party is an 'aggrieved person' under the FISA" (Doc #516/54 at 7) and assert that "the relevant case law makes clear that Congress intended that 'aggrieved persons' would be solely those litigants that meet Article III standing requirements to pursue Fourth Amendment claims." Id at 5. Tellingly, defendants in their reply brief consistently refer to their motion as a "summary judgment motion" and argue that plaintiffs cannot sustain their burden on "summary judgment" based on the allegations of the FAC. Defendants are getting ahead of themselves.

Defendants attack plaintiffs' FAC by asserting that plaintiffs seek to proceed with the lawsuit based on "reasonable inferences" and "logical probabilities" but that they cannot avoid summary judgment because "their evidence does not actually establish that they were subject to the alleged warrantless surveillance that they challenge in this case." Id at 11. At oral argument, moreover, counsel for defendants contended that the only way a litigant can sufficiently establish aggrieved person status at the pleading stage is for the government to have admitted the unlawful surveillance. Transcript of hearing held December 2, 2008, Doc #532 at 5-17.

Without a doubt, plaintiffs have alleged enough to plead "aggrieved person" status so as to proceed to the next step in proceedings under FISA's sections 1806(f) and 1810. While the court is presented with a legal problem almost totally without directly relevant precedents, to find plaintiffs' showing inadequate would effectively render those provisions of FISA without effect, an outcome the court is required to attempt to avoid. See In re National Security Agency, 564 F Supp 2d at 1135 ("While the court must not interpret and apply FISA in way that renders section 1810 superfluous, Dole Food Co v Patrickson, 538 US 468, 476-77, 123 S Ct 1655 (2003), the court must be wary of unwarranted interpretations of FISA that would make section 1810 a more robust remedy than Congress intended it to be.") More importantly, moreover, plaintiffs' showing is legally sufficient under the analogous principles set forth in Alter and In re Sealed Case.

IV

Because plaintiffs have succeeded in alleging that they are "aggrieved persons" under FISA, their request under § 1806(f) is timely. Section 1806(f), discussed at some length in the court's July 2 order (564 F Supp at 1131), is as follows:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Plaintiffs propose several approaches for the court to allow plaintiffs to discover information about the legality of the electronic surveillance under § 1806(f):

\\

> (1) allow plaintiffs to examine a redacted version of the Sealed Document that allows them to see anything indicating whether defendants intercepted plaintiffs' international telecommunications in March and April of 2004 and lacked a warrant to do so;
>
> (2) impose a protective order prohibiting disclosure of any of the Sealed Document's contents;
>
> (3) one or more of plaintiffs' counsel may obtain security clearances prior to examining the Sealed Document (plaintiffs note that precedent exists for this approach, pointing to attorneys at the Center for Constitutional Rights who are involved in Guantanamo Bay detention litigation and attaching the declaration of one such attorney, Shayana Kadidal, describing the process of obtaining Top Secret/Sensitive Compartmented Information ("TS/SCI") clearance for work on those cases (Doc #472-8/46-8)); and
>
> (4) because they have already seen the Sealed Document, plaintiffs' need would be satisfied by the court "simply acknowledging [its] existence and permitting [plaintiffs] to access portions of it and then reference it —— e g, in a sealed memorandum of points and authorities —— in our arguments on subsequent proceedings to determine plaintiffs' standing.

Doc # 472/46 at 27.

In their opposition, defendants do not fully engage with plaintiffs' motion, but rather seem to hold themselves aloof from it:

> [A]side from the fact that plaintiffs have failed to establish their standing to proceed as "aggrieved persons" under the FISA, their motion should also be denied because Section 1806(f) does not apply in this case —— and should not be applied —— for all the reasons previously set forth by the Government. Specifically, the Government holds to its position that Section 1806(f) of the FISA does not preempt the state secrets privilege, but applies solely where the Government has acknowledged the existence of surveillance in proceedings where the lawfulness of evidence being used against someone is at issue.

Doc #499/51 at 24. Defendants have not lodged classified declarations with their opposition as seems to be called for by § 1806(f) upon the filing of a motion or request by an aggrieved person. Defendants, rather, assert that

> The discretion to invoke Section 1806(f) belongs to the Attorney General, and under the present circumstances —— where there has been no final determination that those procedures apply in this case to overcome the Government's successful assertion of privilege and where serious harm to national security is at stake —— the Attorney General has not done so. Section 1806(f) does not grant the Court jurisdiction to invoke those procedures on its own to decide a claim or grant a moving party access to classified information, and any such proceedings would raise would raise serious constitutional concerns.

Id at 26-27, citing Department of the Navy v Egan, 484 US 518, 529 (1988) for the proposition that "the protection of national security information lies within the discretion of the President under Article II)." Of note, the court specifically rejected this very reading of Egan in its July 2 order. See 564 F Supp 2d at 1121.

Defendants simply continue to insist that § 1806(f) discovery may not be used to litigate the issue of standing; rather, they argue, plaintiffs have failed to establish their "Article III standing" and their case must now be dismissed. But defendants' contention that plaintiffs must prove more than they have in order to avail themselves of section 1806(f) conflicts with the express primary purpose of in camera review under § 1806(f): "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." § 1806(f).

In reply, plaintiffs call attention to the circular nature of the government's position on their motion:

> Do defendants mean to assert their theory of unfettered presidential power over matters of national security —— the very theory plaintiffs seek to challenge in this case —— as a basis for disregarding this court's FISA preemption ruling and defying the current access proceedings under section 1806(f)? So it seems.

Doc #515/53 at 17. So it seems to the court also.

It appears from defendants' response to plaintiffs' motion that defendants believe they can prevent the court from taking any action under 1806(f) by simply declining to act.

But the statute is more logically susceptible to another, plainer reading: the occurrence of the action by the Attorney General described in the clause beginning with "if" makes mandatory on the district court (as signaled by the verb "shall") the in camera/ex parte review provided for in the rest of the sentence. The non-occurrence of the Attorney General's action does not necessarily stop the process in its tracks as defendants seem to contend. Rather, a more plausible reading is that it leaves the court free to order discovery of the materials or information sought by the "aggrieved person" in whatever manner it deems consistent with section 1806(f)'s text and purpose. Nothing in the statute prohibits the court from exercising its discretion to conduct an in camera/ex parte review following the plaintiff's motion and entering other orders appropriate to advance the litigation if the Attorney General declines to act.

V

For the reasons stated herein, defendants' motion to dismiss or, in the alternative, for summary judgment (Doc #475/49), is DENIED. Plaintiffs' motion pursuant to 50 USC § 1806(f) is GRANTED (Doc #472/46).

The court has carefully considered the logistical problems and process concerns that attend considering classified evidence and issuing rulings based thereon. Measures necessary to limit the disclosure of classified or other secret evidence must in some manner restrict the participation of parties who do not control the secret evidence and of the press and the public at large. The court's next steps will prioritize two interests: protecting classified evidence from disclosure and enabling plaintiffs to prosecute their action. Unfortunately, the important interests of the press and the public in this case cannot be given equal priority without compromising the other interests.

To be more specific, the court will review the Sealed Document ex parte and in camera. The court will then issue an order regarding whether plaintiffs may proceed —— that is, whether the Sealed Document establishes that plaintiffs were subject to electronic surveillance not authorized by FISA. As the court understands its obligation with regard to classified materials, only by placing and maintaining some or all of its future orders in this case under seal may the court avoid indirectly disclosing some aspect of the Sealed Document's contents. Unless counsel for plaintiffs are granted access to the court's rulings and, possibly, to at least some of defendants' classified filings, however, the entire remaining course of this litigation will be ex parte. This outcome would deprive plaintiffs of due process to an extent inconsistent with Congress's purpose in enacting FISA's sections 1806(f) and 1810. Accordingly, this order provides for members of plaintiffs' litigation team to obtain the security clearances necessary to be able to litigate the case, including, but not limited to, reading and responding to the court's future orders.

Given the difficulties attendant to the use of classified material in litigation, it is timely at this juncture for defendants to review their classified submissions to date in this litigation and to determine whether the Sealed Document and/or any of defendants' classified submissions may now be declassified. Accordingly, the court now directs defendants to undertake such a review.

The next steps in this case will be as follows:

1. Within fourteen (14) days of the date of this order, defendants shall arrange for the court security officer/security specialist assigned to this case in the Litigation Security Section of the United States Department of Justice to make the Sealed Document available for the court's in camera review. If the Sealed Document has been included in any previous classified filing in this matter, defendants shall so indicate in a letter to the court.

2. Defendants shall arrange for Jon B Eisenberg, lead attorney for plaintiffs herein and up to two additional members of plaintiffs' litigation team to apply for TS/SCI clearance and shall expedite the processing of such clearances so as to complete them no later than Friday, February 13, 2009. Defendants shall authorize the court security officer/security specialist referred to in paragraph 1 to keep the court apprised of the status of these clearances. Failure to comply fully and in good faith with the requirements of this paragraph will result in an order to show cause re: sanctions.

3. Defendants shall review the Sealed Document and their classified submissions to date in this litigation and determine whether the Sealed Document and/or any of defendants' classified submissions may be declassified, take all necessary steps to declassify those that they have determined may be declassified and,

no later than forty-five (45) days from the date of this order, serve and file a report of the outcome of that review.

4. The parties shall appear for a further case management conference on a date to be determined by the deputy clerk within the month of January 2009. Counsel should be prepared to discuss adjudication of any and all issues that may be conducted without resort to classified information, as well as those issues that may require such information. Counsel shall, after conferring, submit brief statements of their respective plans or a joint plan, if they agree to one.

IT IS SO ORDERED.

VAUGHN R WALKER
United States District Chief Judge

United States District Court
For the Northern District of California